

Modeling the Impact of Protocols on Traffic Burstiness At Large Timescales in Wireless Multi-Hop Networks

Kaustubh Jain and John S. Baras

The
Institute for
Systems
Research



A. JAMES CLARK
SCHOOL OF ENGINEERING

ISR develops, applies and teaches advanced methodologies of design and analysis to solve complex, hierarchical, heterogeneous and dynamic problems of engineering technology and systems for industry and government.

ISR is a permanent institute of the University of Maryland, within the A. James Clark School of Engineering. It is a graduated National Science Foundation Engineering Research Center.

www.isr.umd.edu

Modeling the Impact of Protocols on Traffic Burstiness At Large Timescales in Wireless Multi-Hop Networks

Kaustubh Jain and John S. Baras
Institute for Systems Research
University of Maryland
College Park, MD 20742
Email: ks Jain, baras@umd.edu

Abstract—We investigate the impact of the protocol stack on traffic burstiness at large time-scales in wireless multi-hop network traffic. Origins of traffic burstiness at large scales (like its LRD nature) have been mostly attributed to the heavy-tails in traffic sources. In wired networks, protocol dynamics have little impact on large time-scale dynamics. However, given the nature of wireless networks, the MAC and routing layers together can lead to route flapping or oscillations even in a static network. Hence, we explore whether these dynamics can lead to traffic burstiness and LRD. Using network simulations, we analyze traffic for two MANET routing protocols - OLSR and AODV. By varying the routing protocol parameters, we analyze their role in inducing or preventing route oscillations, and study their impact on traffic LRD. We find that, losses in OLSR control packets, due to congestion at the MAC, can lead to route oscillations and traffic burstiness at large timescales. By tuning the parameters, route oscillations and traffic LRD can be avoided. AODV dynamics show little evidence for traffic LRD, even though we cannot rule out this possibility. We also show that the route oscillations can have heavier body and tail than exponential distribution, and that the Markovian framework for route oscillations is inadequate to explain the observed traffic scaling. Lastly, we give a model that captures the MAC and OLSR routing protocol interactions and depending upon chosen protocol parameters and input load, correctly predicts the presence of traffic LRD. Thus, we use this model to design appropriate choice of protocol parameters to mitigate traffic burstiness at large-timescales.

I. INTRODUCTION

The existence of self-similarity in Ethernet LAN was established with the seminal work of Leland et al. [1]; self-similarity and the related phenomena of long-range dependence (LRD) characterized the unexpected burstiness and correlation of the network traffic at large-time scales. LRD nature of the traffic has significant impact on network performance through queue-occupancy, service times, packet losses, etc. Existence of LRD also invalidates the use of Poisson arrivals and Markovian queuing analysis. Since then, many works have shown the existence of traffic LRD in various data networks such as ATM, WAN, etc. [2]–[4]. In most of these networks, the high variability in traffic sources, characterized by heavy-tail distributions, has been attributed as one of the main causes of traffic LRD. In particular, heavy-tails in file sizes, connection or flow durations, inter-arrival times, etc.,

have been empirically verified [2], [5], [6]. And, through the fundamental result on *On/Off model* by Taqqu et al. [5], the causal link between heavy-tails and LRD in an idealized setting has been established. Even though idealized, the result and its variations, have been applied with great success in many real-measurements [5], [6] as well as simulation-based studies [7], [8]. The wide applicability of the model in various network settings has led to the belief that the network protocols themselves play little part in the large time-scale behavior of traffic, and that protocol dynamics affect only the small-time scale properties [3], [7], [9], [10].

While the existence of LRD has been widely studied in wire-line networks, there are very few studies in wireless networks [11], [12]. Given the belief that network protocols won't affect large time-scale behavior, it is generally expected that wireless networks will yield similar result. However, we believe, LRD in wireless networks can be qualitatively and quantitatively different, as they include a number of new features such as shared wireless medium, fading as well as mobility. The lower-layer protocols are expected to have more pronounced impact in wireless networks. Also, for multi-hop networks, the routing protocol also plays an important role. Due to variable link conditions in wireless networks, the routing protocol can cause changes in multi-hop routes even in a static topology. The link 'failure' detection mechanisms are different for wireless networks; a certain number of consecutive packet drops is usually used as indicator of link failure, even though these packet drops can be due to fading or congestion. Thus, the wireless medium can introduce route changes which can potentially affect traffic burstiness at large timescales. Hence, we wish to re-examine the impact of protocols on the traffic LRD, in wireless multi-hop networks.

We carry out a simulation-based study to find the relation between traffic burstiness and the impact of protocols in multi-hop wireless networks. In particular, we focus on the role of routing protocols and contention-based MAC on traffic burstiness. We study two routing protocols - OLSR [13] and AODV [14], which are two of the most popular routing protocols for wireless multi-hop networks. While OLSR is a proactive routing protocol, trying to maintain up-to-date topology and

routing information, AODV is a reactive protocol, discovering routes as needed. To keep our focus on the routing protocol and on the wireless MAC, we use idealized physical layer setting (even though we obtained similar results using more realistic channel models). In particular, we observe that losses of routing control packets, at the MAC layer, can lead to route changes even in static networks. Such route changes, in turn, result in bursty traffic at intermediate nodes. Even though, the typical timescale of routing protocol packets is of the order of few seconds, we see that traffic burstiness is observed even at time-scales of up to several hours. Thus, unlike the wired networks studied before, the varying nature of wireless ‘links’ and their impact on routing protocols, result in traffic burstiness at much larger timescales.

Recently, there has been some criticism about the LRD analysis of typically a finitely sampled time-series. At the same time, the impact of LRD traffic on a network with finite buffers is also sometimes questioned. However, irrespective of true LRD or not, traffic burstiness of the order of several hours has practical significance for both the actual network performance as well as network resource provisioning. Our own preliminary experiments show that the performance of contention-based MAC, like 802.11, is affected by the traffic burstiness at large-timescales. Also, LRD or not, the observed traffic oscillations directly impact the carried load in the network. For some of the scenarios, we observed a throughput drop of up to 15 % due to avoidable route oscillations. Hence, it is important to characterize the large-timescale behavior of traffic for more accurate performance evaluation and network design. Otherwise, the actual QoS will be much worse than predicted by traditional models.

For the OLSR scenario, we also model the observed traffic burstiness phenomena using models in two steps. At first, using a simple On/Off packet train model, we explain how route oscillations can lead to traffic burstiness, and how a Markovian framework for route oscillations is not sufficient to explain the large-timescales burstiness. Using a simple 4-node scenario with a single connection, we provide evidence for sub-exponential On and Off durations, providing some evidence for protocol-induced ‘heavy-tails’. Although more experiments are needed for stronger statistical analysis of the observed route oscillation durations, the results presented at the least invalidate the Markovian framework. In the second part, we model the 802.11 MAC and OLSR protocols to show how input traffic load levels can impact protocol dynamics and lead to topology changes even in a static network. For more complicated networks, while we are able to model probability of topology changes, it is difficult to model the exact route oscillations. Hence, we use approximate models to predict the presence of traffic burstiness at large timescales. In particular, we use the 802.11 MAC and OLSR models from [15], to find the probability of some topology changes; thereby, leading to traffic burstiness in at least some of the intermediate nodes. The second model currently does not capture the exact nodes which see route oscillations and traffic burstiness. Lastly, while protocols can lead to traffic burstiness at large-timescale,

appropriate tuning of protocol parameters can mitigate the effect. We use our models to correctly predict what choices of protocol parameters will result in traffic burstiness and what choices will not. Thus, we use the models not just to explain the observed phenomenon, but also to aid in network design.

The paper is organized as follows: In Sec. II, we provide some preliminaries for traffic analysis as well as the relevant protocol dynamics at play in our study. Sec. III includes our preliminary simulation studies which show evidence of traffic burstiness due to OLSR protocol and contention-based MAC. This serves as a motivation for more detailed analysis and modeling. In Sec. IV, we give the details about the On/Off model for route oscillations. Sec. VI, provides a simplistic model linking load-levels, MAC failure probabilities and the resulting impact on OLSR routing. In Sec. VII, we test our models on newer scenarios and demonstrate how we can use them to tune the network parameters appropriately.

II. PRELIMINARIES

A. Traffic Scaling and Wavelet Analysis

To analyze traffic scaling at different time scales, a commonly used statistical tool is based on the Discrete Wavelet Transform (DWT). This has been widely used to study traffic multi-scaling (cf. [9], [16]). The Multi Resolution Analysis (MRA) consists of splitting a given sequence of observations $X = \{X_1 \dots X_n\}$ into the (low pass) *approximation* and the (high-pass) *details* :

$$X = \sum_{k=1}^{n/2^J} a_X(J, k) \phi_{J,k}(t) + \sum_{j=1}^J \sum_{k=1}^{n/2^j} d_X(j, k) \psi_{j,k}(t) \quad (1)$$

where the parameters $\phi_{j,k}(t)$ and $\psi_{j,k}(t)$ are the set of shifted and dilated versions of the scaling function $\phi_0(t)$ and the mother wavelet $\psi_0(t)$. The DWT coefficients are defined as $d_X(j, k) = \langle X, \psi_{j,k} \rangle$ and $a_X(j, k) = \langle X, \phi_{j,k} \rangle$.

The quantity $|d_X(j, k)|^2$ measures the amount of energy in signal X about time $t_0 = 2^j k$ and about the frequency $2^{-j} \lambda_0$ where λ_0 is a reference frequency which depends on the choice of ψ_0 . And the expectation of energy that lies within a bandwidth 2^{-j} around the frequency $2^{-j} \lambda_0$, is denoted by $E[E_j]$ and is approximated by $\frac{1}{n_j} \sum_{k=1}^{n_j} |d_X(j, k)|^2$, where n_j is the number of wavelet coefficients at scale or octave j . The wavelet analysis is widely used to study the Long Range Dependence (LRD) properties of a time-series as well [17]. If X is an LRD process, then the wavelet coefficients satisfy:

$$y_j = \log_2 \left(\frac{1}{n_j} \sum_{k=1}^{n_j} |d_X(j, k)|^2 \right) \sim (2H - 1)j + c, \quad (2)$$

where c is a constant and H is the Hurst parameter which characterizes the degree of LRD. From Eq. (2), a linear regression fit to the plot of y_j against octave j gives an estimate of H . However, to get a good Hurst estimate the region of scaling needs to be carefully identified [8]. Nevertheless, scaling over a finite range of octaves is indicative of traffic burstiness at corresponding timescales. And scaling at higher octaves is a good enough indicator for the presence of LRD.

B. Routing Protocol Dynamics

For multi-hop scenarios, the routing protocol also plays a role in shaping traffic. Depending upon the routing tables, nodes forward traffic to appropriate intermediate hops. Even in a static topology, the routing protocol may change routes due to losses. Loss of routing protocol control packets at the MAC (due to congestion or physical layer losses) can lead to the inference of topology changes. This in turn, can result in route changes even for static topology. Such changes in the routes may lead to additional dynamics in the traffic at each node. One of the main objectives of this study is to analyze the routing protocol dynamics and characterizing the resulting traffic burstiness at large time scales. In our simulations we either use the OLSR [13] or AODV [14] routing protocols. We summarize the details relevant to our study here.

OLSR is a proactive routing protocol. It relies on periodic HELLO and TOPOLOGY CONTROL (or TC) packets to discover local and global topology, respectively. Each node periodically broadcasts HELLO packets (with period T). Whenever a neighboring node receives a HELLO packet, the node assumes that the link to the sender is up. If D consecutive HELLO messages are lost (timed-out), the node infers link failure. Based on the local neighborhood information from HELLO packets, TC packets are broadcast throughout the network, and each node stores its limited view of the global topology. Based on this topology, each node chooses the best next-hop for a given destination. Any changes in local topology, inferred due to HELLO packets, triggers network-wide updates in global topology. Thus, losses in HELLO packets (even due to congestion or fading) can result in changes in inferred topology and hence, the routes. In our scenario, as described before, even though the topology is static and the physical layer errors are zero, periodic HELLO packets could be lost at the MAC layer due to congestion.

AODV is a reactive protocol. Whenever a new connection is created at the source, the source attempts to find the best path to the destination. For a new destination, the source broadcasts Route Request (RREQ) packets which are propagated in the network. The destination node sends out Route Reply (RREP) packets along the best path, using the information stored in the RREQ packets. Once a path has been established, the liveness of the links on the path is determined using both explicit and implicit methods. Explicit methods rely on periodic HELLO packets on the active links. Implicit methods rely on MAC layer ACKs or control messages. Any of these packets could be dropped at the MAC and PHY layers. If none of the explicit or implicit packets are received within a timeout, the node infers link failure and resorts to route recovery.

In OLSR, nodes keep an updated view of the entire topology. In the event of a link failure, nodes will quickly route paths on newer links. If that new path becomes congested later, it might trigger more link ‘failures’. Thus, it is possible that the routes keep oscillating between two paths, leading to traffic burstiness at the intermediate nodes. In AODV, in contrast, nodes only store active routes. In the event of link failure,

there is route recovery. Compared to an OLSR scenario, it is more likely that the route recovery mechanism returns the old path, although route oscillations can occur in AODV as well.

III. SIMULATION STUDY I

At first, we conduct some preliminary experiments to analyze the role of protocol dynamics in shaping traffic at large timescales. This serves as the motivation for a more detailed modeling and analysis that follows.

A. Setup

We used OPNET [18], to carry out our studies of traffic scaling in wireless networks. OPNET is a popular network simulator with well-developed protocol libraries. We studied multi-hop scenarios using IEEE 802.11b MAC (DCF mode). MAC and PHY parameters were set to the standard values. However, to keep our focus on the MAC and higher layers, we set a unit-disc model for the communication range. To achieve this, we used a two-ray ground propagation model, and modified the CCK modulation scheme’s BER curve to be either 0 or 1 depending upon the SNR. Thus, a pair of nodes within a given distance threshold can communicate without any physical layer errors. Also, we disabled the packet-capture mode, implying two or more simultaneous transmissions cause collisions at the receiver, and the packets or frames are discarded. Note that, the use of unit-disc model is only to focus our attention on MAC and Routing. Even though we did not report the results here, we repeated our experiments with realistic PHY and SNR models, to obtain similar results qualitatively.

The source traffic characteristics were specified by the following parameters: 1) *File Size (bytes)*; and 2) *Inter-request Time (sec)* between each file. The traffic applications use TCP/IP protocols (we obtained similar results using UDP). Also, we ran two sets of experiments - one with OLSR and another with AODV. We ran multiple simulations with various distributions assigned to the inputs - application file sizes (packets per request) and inter-request times. In particular, we assigned exponential distributions with varying means to file sizes and inter-request times. Based on the WWW file size traces from [2], we used the mean file size of 13715 Bytes. By changing the mean inter-request time, we varied the load on the network. Even though these parameters were changed across simulations, all the connections used the same distribution for a particular simulation run. For each of the scenarios studied below, we ran each simulation for 1 day. At each node, we measured the MAC layer throughput every $\Delta = 0.1$ sec. Thus, this captures the actual load on the network, as compared to application-level traffic traces available only at the source and destination nodes. We also measured buffer losses, and losses due to the retry limit threshold at the MAC, for making inferences about the load-level and the role of the MAC. We ran our traffic analysis study on the traffic received MAC layer. While processing the results, we discarded the initial 15 minutes of data to remove transients. This is enough time even for initial route setup.

We used a 30-node topology as shown in Fig. 1(a). The lines between the nodes indicate communication links. We set several source-destination pairs: $2 \leftrightarrow 4$, $3 \leftrightarrow 10$, $5 \leftrightarrow 7$, $6 \leftrightarrow 8$, $12 \leftrightarrow 17$, $13 \leftrightarrow 20$, $15 \rightarrow 18$, $18 \rightarrow 19$, $22 \leftrightarrow 23$, $24 \leftrightarrow 29$, $26 \rightarrow 24$, $30 \rightarrow 21$, $1 \leftrightarrow 21$, $11 \rightarrow 2$, $19 \rightarrow 2$. There are multiple short connections within the clusters, but there are some connections across the clusters as well.

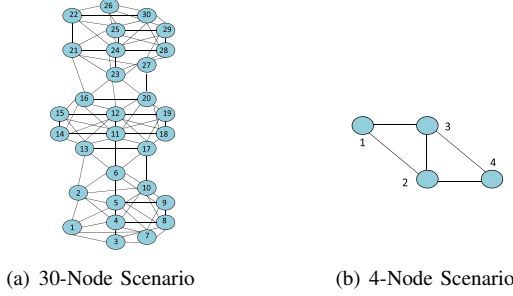


Fig. 1. Simulated Topologies

To study the impact of routing protocols, we ran two sets of simulations - one each with OLSR and AODV protocols. We initially chose the default parameters according to the respective RFCs. However, as we will see later (see Sec. III-B), route oscillations were clearly visible in OLSR scenarios (and not so obvious for AODV). In our simulations, since the physical layer errors are zero, the loss of routing packets at the MAC layer are purely due to congestion and collision. To study the OLSR route oscillations in more detail, we tuned the OLSR routing parameters as described in Sec. III-C. But first, we describe the results for the default parameters.

B. Impact of Routing Protocols

We used exponential file size distributions (with mean 13715 Bytes) and exponential inter-request time, with mean 2 sec (for medium load) or 10 sec (for low load). For medium load (mean inter-request time = 2 sec), the total offered load was around 1.5Mbps. While it is difficult to characterize the capacity of the network, we call the load-level medium, because, for properly tuned routing protocols (as described later), all of the offered load was carried by the network. Even for the default OLSR scenario, the throughput was 99.6%.

Fig. 2 shows the wavelet analysis for the traffic successfully received at the MAC layer of a sample Node 25 (measured in bps). On the x-axis, octave j corresponds to $t = 2^j * \Delta$, where $\Delta = 0.1$ seconds. Thus, $octave\ j = 10$ implies $t = 100$ seconds. Scaling at large timescales is indicative of traffic LRD. Fig. 2(a) shows that, the traffic at the intermediate Node 25 displayed LRD, when using the OLSR routing protocol. For exactly the same parameters, but using AODV, there was no clear evidence of traffic LRD (see Fig. 2(c)). We made similar observations for low load scenarios. While we may debate whether the finite series is actually LRD or is 'pseudo-LRD', the traffic is definitely bursty at scales from hundreds of seconds to several hours. Thus, to the best of our knowledge, unlike any other previous study, our simulations show for the first time that wireless network protocols can impact traffic at

large timescales for several hours. This impacts the network performances as discussed before. For the sake of brevity, we call this traffic burstiness as traffic 'LRD' in the following discussions, although 'pseudo-LRD' will be more appropriate.

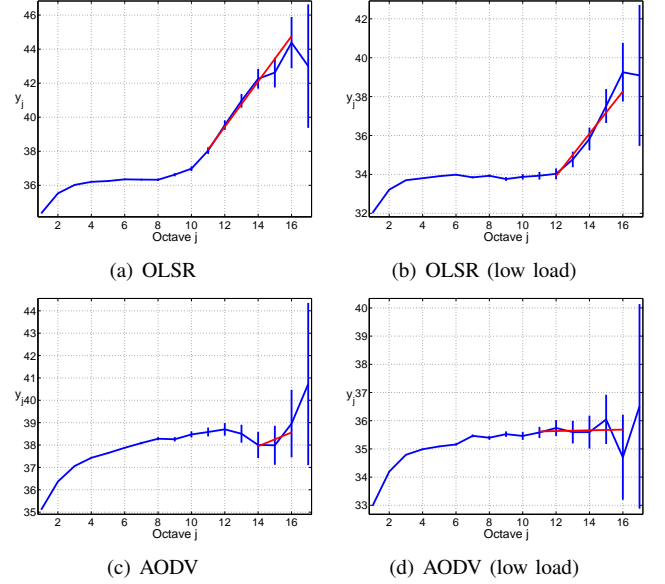


Fig. 2. LRD due to Routing Protocol

Clearly, the LRD in traffic at intermediate nodes was due to the OLSR routing protocol. To inspect this in more detail, Fig. 3 shows the time series plot for aggregate traffic (sent from all the sources combined) as well as the traffic at node 25. The plots are for the scenario with low load (mean inter-request time = 10 sec). Clearly, Fig. 3(b) shows that there were periods of very low traffic at node 25 when using OLSR. During the times when node 25 was carrying less traffic, neighboring nodes (especially node 24) carried more traffic (Fig. 3(c)). These results are strong evidence of route oscillations, in OLSR, leading to traffic LRD. At least for the scenarios studied, AODV induced little traffic burstiness.

C. Impact of OLSR Parameters

To further study the impact of the OLSR protocol in inducing traffic LRD, we changed the OLSR protocol parameters. In OLSR, the default values of T is 2 sec, and D is 3 (Sec. II-B). That is, if $D = 3$ consecutive HELLO messages are lost (timed-out), the node infers link failure, which results in topology and route updates. In our scenario, as described before, even though the topology is static, periodic HELLO packets may be lost at the MAC layer. In the scenarios studied above, we observed evidence for the same. To test our hypothesis that route changes are due to drops of consecutive HELLO packets, we set $D = 10$. Hopefully, the probability of 10 consecutive packet drops (spread over $T * D = 20sec$) is low enough to avoid unnecessary route updates. We reran our simulation and analysis for the scenarios as above with $D = 10$ for OLSR. We denote these scenarios as *Tuned-OLSR*, to differentiate them from the (untuned) OLSR

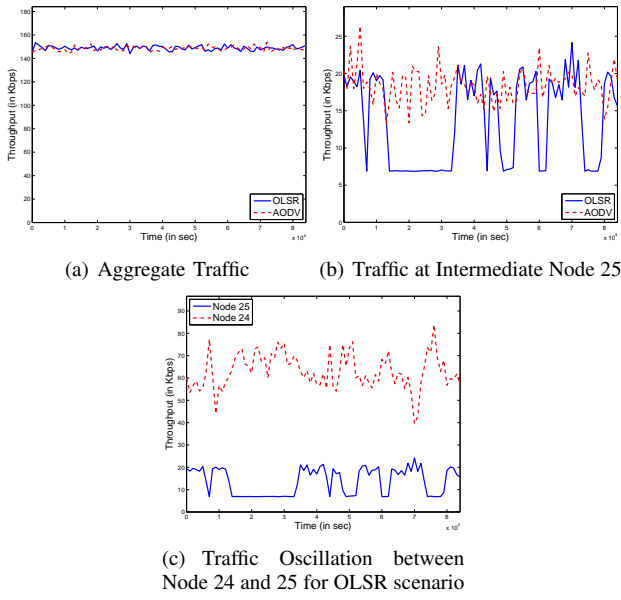


Fig. 3. Evidence of Route Oscillations in OLSR scenario

scenarios before. Fig. 4 shows that there was no LRD in traffic. The figure shows the traffic at Node 25, but all other nodes showed similar behavior. Also, there were no route or topology updates after the initial setup time. Clearly, by tuning the OLSR parameters, unnecessary route oscillations were avoided. This in turn, leads to absence of routing-protocol-induced LRD. Note, even though this choice of high D avoided route oscillations in our scenario, other consequences include high delay in detecting true link failures, say, due to mobility.

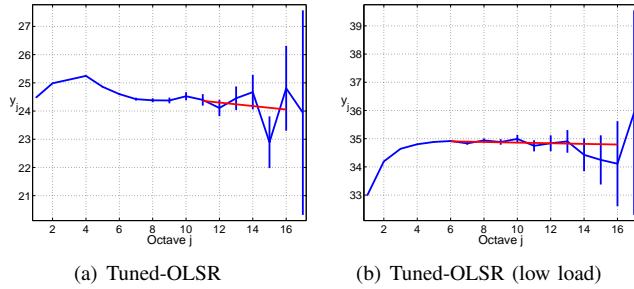


Fig. 4. Parameter tuning in OLSR to avoid route oscillations and traffic LRD

IV. MODELING TRAFFIC BURSTINESS DUE TO ROUTE OSCILLATIONS

In this section, we attempt to relate the observed traffic burstiness at large timescales to the presence of route oscillations. We attempt to model the route oscillations using a simply On/Off packet train model and use it to explain the observed traffic scaling.

1) *Analysis of Simple 4-node Topology:* We start with a simple topology (Fig. 1(b)). Nodes 1 and 4 are the source and destination. Nodes 2 and 3 forward traffic depending upon routes chosen by the protocols. OLSR will typically select route $1 \rightarrow 2 \rightarrow 4$ or else $1 \rightarrow 3 \rightarrow 4$. However, due to

intermittent link losses of OLSR Control Packets, OLSR can infer the topology incorrectly. Hence, the chosen route (and forwarded traffic) oscillates between the two paths. For the intermediate nodes, then, the traffic at its MAC layer depends on the chosen route at the source. And hence, incoming traffic can be modeled using an On/Off model packet train model. Since we are focusing on the large time-scale behavior, we can ignore the small time-scale dynamics (due to the source and the MAC layer). Hence, we assume a constant traffic rate during the On periods and no traffic during the Off periods.

We measured the traffic at intermediate nodes (2 and 3) and analyzed their scaling properties. Fig. 5 shows a few sample plots indicating a strong presence of traffic burstiness at large timescales. In particular, the high (low) load scenario corresponds to mean inter-arrival time was 0.06 seconds (0.8 seconds). We observed similar behavior for different load levels.

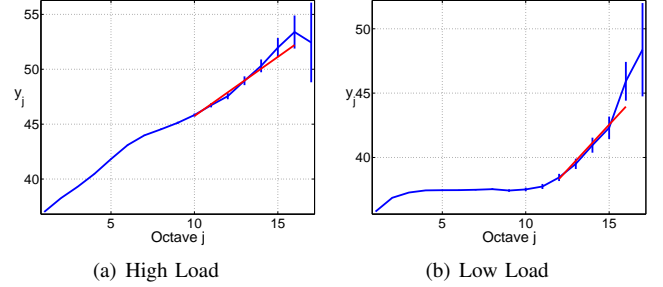


Fig. 5. Timescale of Traffic Burstiness in 4-Node Scenario

We also measure the actual route chosen and from that deduce the On / Off durations distribution for traffic at the intermediate nodes. So, whenever node 2 is present on the chosen path, it corresponds to the On duration. And when the chosen path is $1 \rightarrow 3 \rightarrow 4$, it corresponds to the Off duration for node 2. Then, using the On / Off Model, we attempt to predict the traffic burstiness. Initially, motivated by the usual Markovian framework, we assumed i.i.d. Exponential distributions for the On and Off Durations with appropriate mean (17.48 and 23.67, respectively) corresponding to the observed values. Fig. 6(b) shows that the Markovian model for route oscillations cannot explain the observed traffic burstiness (Fig. 6(a)) at large timescales of several hours, which is 3-4 orders of magnitude higher than the mean. However, if we use the empirical distributions, the prediction about traffic scaling is accurate (Fig. 6(c)). Note that, Fig. 6 uses $\Delta = 1$ (unlike $\Delta = 0.1$) seconds as the sampling interval, hence the shift in the x-axes.

We investigated the On and Off distributions more carefully. In Fig. 7, we plot the On and Off duration distributions for the high load scenario (mean inter-arrival time of 0.06 seconds). It shows the CCDF and quantile-quantile (QQ) plot for the On and the Off (empirical) distributions compared to exponential distributions with respective means. As can be seen, the On durations have much heavier-body, and slightly fatter tail compared to the exponential. Note that the CCDF plot is on a log-log scale. Repeated experiments with different load conditions

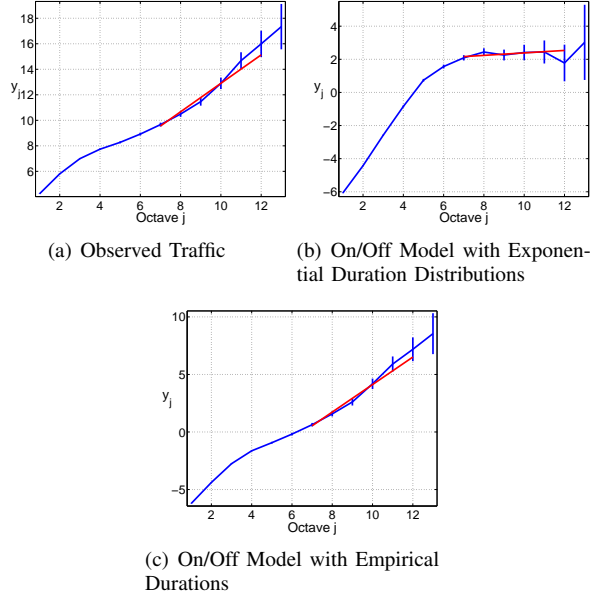


Fig. 6. On/Off Model and Traffic Burstiness

and different random seeds yielded similar observations. These observations are in line with sub-exponential tails leading to much higher lag in correlations, or burstiness at much higher scales. Whether the empirical distributions are true heavy-tails or not, needs more detailed evaluation.

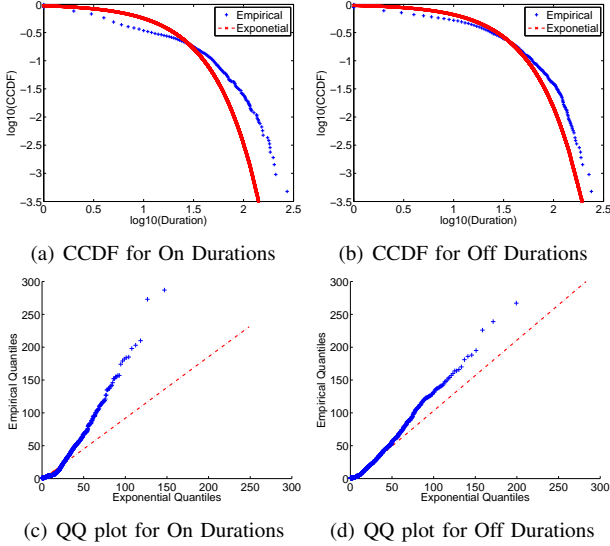


Fig. 7. Empirical On and Off Durations Distribution Compared With Exponential

V. MODELING THE MAC COLLISIONS AND OLSR LINK FAILURES

A. MAC Model

Starting with the seminal work by Bianchi et al. [19], there are some works [20]–[23] in throughput modeling for networks using 802.11 MAC. They are abstract MAC models for estimating the average transmission attempt rates, collision

rates, service times and throughput. They model the detailed working of the collisions and back-offs to get good approximations to average throughput. Below, we give a brief overview of our model introduced in [24] and improved in [23].

Given the topology and input traffic load λ on each connection, we model the MAC protocol and attempt to find its performance parameters. The output parameters include link loss probabilities, attempt rates, service times and carried loads. We denote by $\beta_{i,p}$, the probability of MAC layer transmission failure of path p packet at node i . $\theta_{i,j}$ is the probability of transmission from node i neighbors that are hidden from node j . We denote the arrival rate of the path p packets at node i by $\lambda_{i,p}$, and corresponding service times by $T_{i,p}$. From various $\lambda_{i,p}$, we can obtain the connection and network throughput. In obtaining the above parameters, we assume the topology and the average input loads do not change till the system reaches steady-state and time averages converge. We also assume that the packet errors are independent and not bursty.

Assuming that node accesses the channel with a fixed probability α'' when the channel is free. Then, conditioned on the event that node i is scheduled to serve a packet on path p :

$$\alpha''_{i,p} = \frac{2(1-2\beta)(1-\beta^{m+1})}{(1-2\beta)(1-\beta^{m+1}) + W(1-\beta)(1-(2\beta)^{m+1})} \quad (3)$$

where m is the MAC retransmission limit and W is the minimum back-off window and $\beta = \beta_{i,p}$. The above equation is derived by applying renewal-reward theorem. Taking the renewal cycle as total back-off time for a particular packet and the rewards as number of transmission attempts, [20] derive the above relation.

Now, the average serving time of a path p packet at node i , $T_{i,p}$, consists of 4 components as follows:

- $s_{i,p}$: average time for successful transmission of path p packets at node i .
- $b_{i,p}$: average back-off time of node i .
- $u_{i,p}$: average time for successful transmission to and from node i neighbors.
- $c_{i,p}$: average time of unsuccessful transmission due to PHY layer errors and collisions at the MAC layer in the neighborhood of node i .

Thus,

$$T_{i,p} = s_{i,p} + b_{i,p} + u_{i,p} + c_{i,p} \quad (4)$$

The probability of successful transmission of a packet of path p at node i is $(1 - \beta_{i,p}^m)$. And successful transmission time for a packet is $\tau_P = T_{RTS} + SIFS + T_{CTS} + SIFS + T_P + SIFS + T_{ACK} + DIFS$. Hence, the first component is,

$$s_{i,p} = (1 - \beta_{i,p}^m)\tau_P \quad (5)$$

Let CW_j be the back-off window size at stage j , then $W_j = CW_j/2$ is the average back-off time at stage j and the average back-off time is,

$$b_{i,p} = \sum_{j=0}^m W_j \beta_{i,p}^j \quad (6)$$

Algorithm 1 FPA Model

```
1: Initialize: ( $\underline{\beta}, \underline{X}$ )
2: while  $\underline{\beta}$  is not converged do
3:   while  $\underline{T}$  is not converged do
4:      $\underline{X}^{new} = F_{\underline{X}}(\underline{X}, \underline{\beta})$ 
5:      $\underline{X} = \underline{X}^{new}$ 
6:   end while
7:    $\underline{\beta}^{temp} = F_{\underline{\beta}}(\underline{X})$ 
8:    $\underline{\beta}^{new} = \epsilon \underline{\beta}^{temp} + (1 - \epsilon) \underline{\beta}$ 
9:    $\underline{\beta} = \underline{\beta}^{new}$ 
10: end while
```

The remaining two components, $u_{i,p} = f_1(\alpha'', \beta, \underline{Z})$ and $c_{i,p} = f_2(\alpha'', \beta, \underline{Z})$ are some complicated functions of the attempt rates and the collision probabilities, and other auxiliary variables \underline{Z} . Please refer to [23] for more details.

Lastly, the link failure probability depends upon the attempt rates of neighbors. For the purpose of explaining the intuition, let's assume there are $n - 1$ neighboring links, and all the links have similar attempt rates, α'' . The attempt rates are conditioned on the respective transmitting node attempting to serve a packet, where λT is the average queue occupancy. Then the link failure probability is given by

$$\beta = 1 - (1 - \alpha'' \lambda T)^{n-1} \quad (7)$$

The equation for $\beta_{i,p}$ under non-homogeneous conditions is given in [23].

Thus, the above equations describe the relations between various model parameters. However, they are defined iteratively. We use a fixed-point algorithm to find a consistent solution for the given set of non-linear equations. Let \underline{Y} be the set of parameters and $\underline{F}(\underline{Y})$ be the set of equations that express the average system behavior by approximating each parameter in terms of the other parameters. One common way to find a solution to the given set of equations is to use fixed point iterations,

$$\underline{Y}^{new} = \underline{F}(\underline{Y}) \quad (8)$$

A single-loop fixed point algorithm oscillate or converges to unrealistic values because of the implicit dependence of losses at a node and service times of its neighboring nodes. Hence, we use a two-step algorithm to find link losses and service times. First, we fix β , and run a fixed point algorithm to find the service times T , and other parameters. Then, using these parameters, we update β . Hence, we update the parameters iteratively in two nested loops as follows:

Let \underline{X} be the set of parameters excluding $\underline{\beta}$ and $F_{\underline{X}}(\underline{X}, \underline{\beta})$, and $F_{\underline{\beta}}(\underline{X})$ be the set of equations that are derived to approximate \underline{X} , and $\underline{\beta}$ respectively. The iterative algorithm is described in the pseudo code in Algorithm 1. The inner while loop updates \underline{X} parameters using a fixed point iteration. The outer loop updates $\underline{\beta}$ using a convex combination (weighted average) of previous and new value, where ϵ specifies the weight. The convergence criteria in both cases is based on the maximum difference in old and new computed values of

the specified parameters, which is $\underline{\beta}$ for the outer loop and \underline{T} for the inner loop.

Thus, given the input load, the *MAC model* approximates the average MAC frame drop probabilities over various links. We use these MAC frame drop probabilities as the probability of OLSR control packets losses, which form the input to our *OLSR model*, described in the Sec. V-B.

B. OLSR Model

Here, we present a model for the working of OLSR route calculations. In particular, given the packet transmission failures (MAC frame drop probabilities), our model tries to find out the probability of topology change (and route recalculations). For this, we use the component-based performance models developed in [25] and [26]. However, we modify the models for our new metric of interest: the probability of topology changes. The model is described as follows.

The Neighbor Discovery Component (NDC) of OLSR is responsible for detection of changes in a node neighborhood. A node is said to be a neighbor of another node if there exists a bidirectional communication link between them. The link is bidirectional if communication in both directions is possible. Node $k \neq i$ is said to be the second order neighbor of i , if it is not a neighbor (or first order neighbor) of i , but it is a neighbor of one of node i 's neighbors.

NDC relies on periodic transmission of HELLO messages for detection of first and second order neighbors. A HELLO message from node i contains the transmitting node's ID, the list of detected nodes by node i , and the status of the links (directional or bidirectional) between node i and its detected nodes. Thus, from the received HELLO messages a node can detect its first and second order neighbors. When a node j receives a HELLO message from node i that contains its own ID, it will add node i to its neighbor list. Node j removes i from its neighbor list if it does not receive any HELLO message from i for the Neighbor Hold Time (NHT) period.

While HELLO messages help in detecting bidirectional neighbors, this local information about bidirectional links is flooded through out the network using TOPOLOGY CONTROL messages. The controlled flooding for TOPOLOGY CONTROL messages along with the HELLO messages, help nodes to construct a global view and discover routes. Thus, any change in the bidirectional link state of any link may result in global topology changes.

We model the NDC as a Finite State Machine (FSM), so that we can use Markov chain methods to derive the desired steady state probabilities for NDC. A simple Markov chain model for the link between nodes i and j is depicted in Figure 8. The parameter s_{ij} is the probability of success in sending HELLO messages and f_{ij} is the probability of failure. In states U to $U + D - 1$, NDC considers that the link is UP (DU) and node i will add j in its HELLO messages; in states 1 to $U - 1$ and state $U + D$ the link is DOWN (DD). Suppose that we are initially at state $U + D$; only after U subsequent successful reception of HELLO messages we move to state U , and a directional link is declared detected. Similarly, when we are

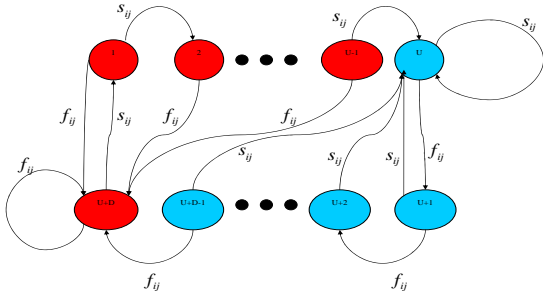


Fig. 8. Markov chain model for the neighbor discovery mechanism

in state U , there should be D subsequent failures in reception of HELLO messages before a directional link is removed from the list.

The design (or control) parameters for NDC are the U and D parameters that can be set to achieve the desired performance. In OLSR, the value of U is fixed to 1, since after the reception of only one HELLO message, the recipient assumes that a directional link exists, and after receiving a HELLO message which contains the recipient ID, it declares that there is a bidirectional link. Therefore, in OLSR we can only control the D parameter by changing NHT. When $U = 1$, the FSM state $U - 1$ is same as the state $U + D$.

Let π_k be the steady state probability that NDC is in state k of the Markov chain. We can use the generalized global balance equations to derive the steady state probabilities. The details are given in [25]. Then, the probability of detecting a directional link to node j at node i is:

$$q_{ij} = \sum_{k=U}^{U+D-1} \pi_k, \quad (9)$$

where π_k and q_{ij} are functions of s_{ij} and f_{ij} .

We assume that the probability of successful transmission from i to j and from j to i are independent from each other. Then the two FSMs at nodes i and j (for directional links $j \rightarrow i$ and $i \rightarrow j$, respectively), can be assumed to be independent. Then the bidirectional link state is UP (BU) if both FSMs are in directional UP states (UU). Thus, the probability of a bidirectional link detection is:

$$p_{ij} = q_{ij} \cdot q_{ji}. \quad (10)$$

Next, focusing on the most susceptible link, we take $f_{ij} = f_{ji} = \beta_{max}$ (from *MAC model* of Sec. V-A).

For the sake of brevity, we assume $f_{ij} = f_{ji} = f$ and drop the subscripts i and j for the remaining derivations. The general case when $f_{ij} \neq f_{ji}$ is a simple extension. The probability of change of bidirectional link status is then given by:

$$p_{change} = p_{BU \rightarrow BD} \cdot p + p_{BD \rightarrow BU} \cdot (1 - p) \quad (11)$$

where

$$p_{BU \rightarrow BD} = \frac{2\pi_{U+D-1} \cdot f \cdot q}{p}$$

is the probability of transition from bidirectional UP state (BU) to bidirectional DOWN state (BD). This happens when both of the FSMs are in directional UP states (DU), and one of them makes a transition to states DD .

And,

$$p_{BU \rightarrow BD} = \frac{2\pi_{U-1} \cdot s \cdot q + \pi_{U-1}^2 \cdot s^2 - 2\pi_{U-1}\pi_{U+D-1} \cdot s \cdot f}{1 - p}$$

is the probability of transition from BD to BU . This happens when: i) one of the FSM is in states DU and the other makes a transition from DD to DU ; or ii) when both the FSM simultaneously transition from DD to DU ; but not when iii) one of the FSM transitions from DD to DU , but the other transitions from DU to DD .

Thus, $p_{change}(f)$ gives the probability of state change for a particular link, as a function of its MAC layer frame drop probability f . Change in any link status may results in global topology change and may lead to route calculations. Since, route recalculations are performed at every fixed intervals and aggregated for all link changes, we make another approximation. We assume that the probability of topology change (ν) is dominated by the probability of link status change of the most susceptible link. Hence, we assume $\nu = p_{change}(\beta_{max})$, where β_{max} is obtained from the *MAC model* described previously.

VI. MODELING ROUTE OSCILLATIONS DUE TO MAC LOSSES

In this section, we aim to validate our model to predict when route oscillations may occur in a large topology, when using OLSR. We present the results here to demonstrate that the MAC and routing protocol dynamics are the origins for the observed traffic burstiness, and also this traffic burstiness can be mitigated by appropriate parameter choices. In this section, we will call the abstract model for 802.11 as the *MAC model*, and the topology / routing change model as the *OLSR model*. The *MAC model* takes the offered load level and topology as inputs to predict MAC frame drop probabilities for various links. The *OLSR model* uses these MAC loss probabilities as input to give topology change probability and predict route oscillations. Thus, in this section, we use our models to connect input load levels, with MAC packet drops and OLSR topology and routing changes. We use the 30-node topology to validate our models, and also demonstrate how we can design the protocol parameters to avoid traffic LRD.

A. Modeling: Link Losses and Topology Changes

1) *Packet Collisions due to Increasing Load Levels*: At first, using the *MAC model* for 802.11, we find the MAC packet or frame drop probabilities depending upon the input load level. Depending upon the topology and different traffic demands, each wireless 'link' will have varying probability for MAC frame drop due to collisions. OLSR HELLO packets will suffer losses according to these probabilities. Since more MAC loss probability leads to more dynamism in OLSR link changes, the overall rate of OLSR topology changes will be

mainly governed by the most susceptible link. Hence, amongst all the different links, we consider the link with highest MAC layer losses (as input to the OLSR model). In Fig. 9(a), we show the maximum (over links) average (over time) MAC failure probability as a function of input load. Clearly, as the load increases, there are more collisions at the MAC level.

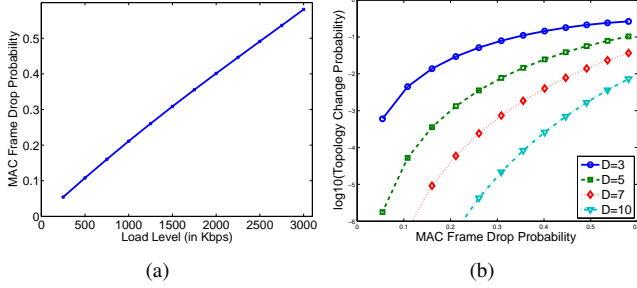


Fig. 9. Load Level, MAC Losses and OLSR Topology Change Probabilities

2) *OLSR Link Failures due to Packet Collisions:* Now, using the maximum MAC failure probability as an input to *OLSR model*, we obtain the steady-state probability of OLSR link changes in the most susceptible link. Note that any local change in topology is likely to result in global topology changes and routes calculations. Also, changes at different links are aggregated and sent periodically. Hence, even if two links change in a slot, only one update will be propagated network wide. Thus, the rate or probability of OLSR topology changes (globally) is mainly determined by the rate of link status change of the most susceptible link. Hence, we assume that the *OLSR model* output gives the probability of global route table calculations (see Sec. ?? for more details). Using the *OLSR model*, Fig. 9(b) shows the probabilities of OLSR topology changes as a function of MAC loss probabilities, for various choice of OLSR parameter D . As conjectured in Sec. III-C, higher D mean more resilience to MAC layer losses.

We compare the OLSR model output with actual statistics obtained from OPNET simulations. For a given value of OLSR parameter D , Fig. 10 shows the model and OPNET probabilities of topology changes (and resulting route re-calculations), for various load-levels (normalized to 1 for maximum load of 3 Mbps). The topology change probabilities from OPNET are obtained as the fraction of instances when HELLO message exchanges (slotted) lead to topology changes. The y-axes are truncated to hide low data points. Also the missing data points for the OPNET dataset corresponds to $\log(0)$. The model output matches very closely with the OPNET results. There is some mismatch at higher levels of MAC loss probabilities, especially for $D = 3$. We believe that is due to the assumption about the most susceptible link dominating the network-wide topology changes. However, even other links can increase the topology change rate, and their impact can be higher at higher MAC loss levels. Nevertheless, the model predicts the order of topology change probability correctly.

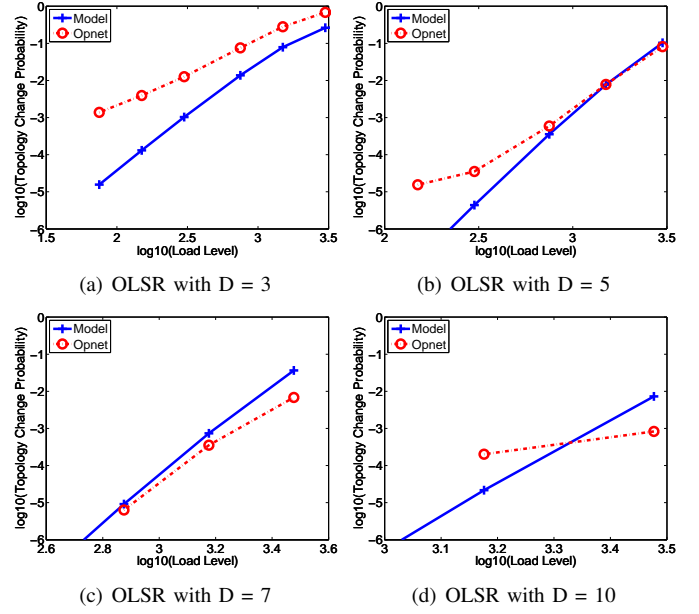


Fig. 10. OLSR Topology Changes due to Increasing Load Levels

Load (in Kbps)	75	150	300	750	1500	3000
D=3	0	1	1	1	1	1
D=5	0	0	0	0	0.3	1
D=7	0	0	0	0	0	0.2
D=10	0	0	0	0	0	0
AODV	0	0	0	0	0	0

TABLE I
LRD AT NODE 25 FOR DIFFERENT LOAD LEVELS IN 30-NODE SCENARIO

B. Analysis: Traffic LRD

1) *Traffic Burstiness due to OLSR Topology Changes:* Next, we turned our attention back to traffic burstiness and wavelet analysis. We ran wavelet analysis on traffic at intermediate nodes (as in Sec. III). For each value of D and different load-levels, we ran the simulation for 1 day, and repeated the experiment with 5 different random seeds. As before, we present the sample results for central node 25. However, instead of showing the numerous wavelet plots, we just list the results in Tab. I. The table should be read as follows: the value give the fraction of scenarios (out of the 5 random seeds), in which we observed traffic LRD according to the wavelet analysis. Clearly, we see that for low values of D , collisions at the MAC couple with OLSR to give rise to traffic LRD. And as we increase D , such traffic burstiness can be avoided. The last row also shows the results for AODV, validating the absence of traffic burstiness in any of the AODV scenarios.

Combining the topology change probabilities from the *OLSR model* and observed LRD in traffic, we look at traffic LRD as a function of topology change probabilities. In Fig. 11, shows the fraction (out of 5 random seeds) of scenarios where traffic was LRD at Node 25 (irrespective of the value of D). Thus, there is a strong correlation between topology change and traffic LRD.

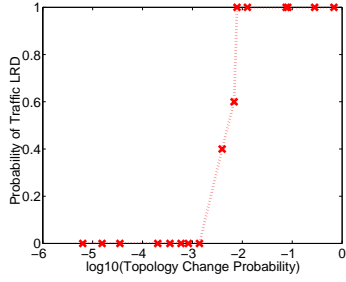


Fig. 11. Traffic LRD with Topology Change Probability Estimate from the Model

VII. NETWORK DESIGN AND VALIDATION

This section serves two purposes: to give additional evidence for traffic LRD; and to illustrate the design methodology. We, thus, validate the models and their utility in choosing an appropriate value for OLSR design parameter D to avoid traffic LRD. For these purposes, we use the topologies shown in Fig. 12. For the 25-node scenario, we setup three connections: $1 \rightarrow 20$, $5 \rightarrow 18$ and $18 \rightarrow 25$. For the 10-node scenario, we setup 10 connections: $1 \rightarrow 9$, $2 \rightarrow 7$, $3 \rightarrow 10$, $4 \rightarrow 5$, $5 \rightarrow 1$, $6 \rightarrow 8$, $7 \rightarrow 4$, $9 \rightarrow 6$, $10 \rightarrow 3$.

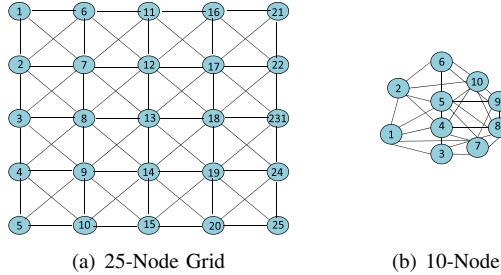


Fig. 12. Other Topologies

We use our model to justify a choice of design parameter D . In particular, given the topology and traffic demands, we rely on our model to find: 1) the MAC failure probability, and 2) Topology change probability, for a given choice of D . If the probability of topology change is non-negligible, then we should see traffic LRD at least in some nodes (as in Fig. 11). Hence, the particular choice of D is not suitable. Tab. II and Tab. III give the results for 25-node and 10-node scenarios respectively. They show the model outputs - the MAC loss probabilities and topology change probabilities, for different input load levels and design choice D . Then, the last row also gives the presence (or absence) of traffic LRD as observed from simulation traces. The table, and Fig. 11, show that the model correctly predicts which values of D will give rise to traffic LRD and which won't. In particular, if the topology change probability is too low, traffic will not be LRD. For high probability of topology change, traffic will be LRD (in atleast some of the intermediate nodes). The only exception seems to be at load level of 0.1 with $D = 3$. According to the model, the probability of topology change is negligible and hence we should not have observed traffic LRD. However,

Load (in Kbps)		36	360	720	1200	1800
MAC Failure Probabilities		0.0219	0.2190	0.4152	0.6354	0.6913
Topology Change Probability	$D=3$	$4.1e-5$	0.032	0.155	0.278	0.273
	$D=10$	$9.9e-17$	$7.9e-7$	$3.5e-4$	0.015	0.03
	$D=20$	$2.5e-33$	$2.0e-13$	$5.4e-8$	$1.6e-4$	$7.6e-4$
Traffic LRD	$D=3$	0.2	1	1	1	1
	$D=10$	0	0	0	0.1	1
	$D=20$	0	0	0	0	0

TABLE II
ANALYSIS FOR 25-NODE SCENARIOS

Load (in Kbps)		120	1200	2400
MAC Failure Probabilities		0.0471	0.4303	0.7517
Topology Change Probability	$D=3$	$3.9e-4$	0.167	0.242
	$D=10$	$2.0e-13$	$4.9e-4$	0.053
Traffic LRD	$D=3$	1	1	1
	$D=10$	0	0	1

TABLE III
ANALYSIS FOR 10-NODE SCENARIOS

we do see traffic LRD. We believe this is because of the approximations of the model which seem to be inaccurate for low load levels and low value of D (similar to the mismatch in Fig. 10(a)). Thus, the model predicts the possibility of traffic LRD accurately. And we can use the model to chose the right D .

VIII. CONCLUSIONS

We explored the impact of routing protocols in large time-scale traffic burstiness. In particular, we observed that packet losses at the MAC (even due to congestion) can lead to route oscillations in OLSR. Route oscillations, in turn, lead to traffic burstiness at large timescales and LRD. We showed that protocols in wireless multi-hop networks can induce traffic burstiness at timescales much larger than previously thought. We also show that the route oscillations are not accurately modeled by relying on Markovian models for exponential durations. Lastly, we also used performance models for 802.11 MAC and OLSR routing, to correctly predict the MAC losses due to input load, and resulting route oscillations and traffic burstiness. Thus, using these models, we can design the network settings to avoid such phenomena.

ACKNOWLEDGMENT

Research supported by the Army Research Office under MURI award W911NF-08-1-0238 and by the National Science Foundation under grant CNS1018346.

REFERENCES

- [1] W. E. Leland, M. S. Taqqu, W. Willinger, and D. V. Wilson, "On the self-similar nature of ethernet traffic (extended version)," *IEEE/ACM Transactions on Networking*, vol. 2, no. 1, pp. 1–15, 1994.
- [2] M. E. Crovella and A. Bestavros, "Self-similarity in world wide web traffic: Evidence and possible causes," *Performance Evaluation Review*, vol. 5, no. 6, pp. 835–846, 1996.
- [3] K. Park and W. Willinger, Eds., *Self-Similar Network Traffic and Performance Evaluation*. John Wiley & Sons, 2000.
- [4] O. I. Sheluhin, S. M. Smolskiy, and A. V. Osin, Eds., *Self-Similar Processes in Telecommunications*. Wiley & Sons, 2007.
- [5] W. Willinger, M. S. Taqqu, R. Sherman, and D. V. Wilson, "Self-similarity through high-variability: statistical analysis of ethernet lan traffic at the source level," *IEEE/ACM Transactions on Networking*, vol. 5, no. 1, pp. 71–86, 1997.

- [6] V. Paxson and S. Floyd, "Wide area traffic: the failure of poisson modelling," *IEEE/ACM Transactions on Networking*, vol. 3, no. 3, pp. 226–244, 1995.
- [7] K. Park, G. Kim, and M. Crovella, "On the relationship between file sizes, transport protocols, and self-similar network traffic," in *International Conference on Network Protocols (ICNP)*, 1996, pp. 171–180.
- [8] P. Abry, P. Borgnat, F. Ricciato, A. Scherrer, and D. Veitch, "Revisiting an old friend: on the observability of the relation between long range dependence and heavy tail," *Telecommunication Systems*, vol. 43, no. 3-4, pp. 147–165, 2010.
- [9] H. Jiang and C. Dovrolis, "Why is the internet traffic bursty in short time scales," in *ACM Sigmetrics*, 2005, pp. 241–252.
- [10] Y. Sumida, H. Ohsaki, M. Murata, and H. Miyahara, "Effects of upper-layer protocols on the self-similarity of network traffic," *Electronics and Communications in Japan (Part II: Electronics)*, pp. 272–279, 2001.
- [11] J. Yu and A. P. Petropulu, "Is high speed wireless network traffic self-similar?" in *IEEE International Conference on Acoustics, Speech and Signal Processing*, 2004, pp. 425–428.
- [12] M. Gidlund and N. Debernardi, "Scheduling performance of heavy-tailed data traffic in wireless high-speed shared channels," in *Wireless Communications & Networking Conference*, 2009, pp. 1818–1823.
- [13] T. Clausen and P. Jacquet, "Optimized Link State Routing (OLSR)," in *IETF RFC 3626*, 2003.
- [14] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," in *IETF RFC 3561*, 2003.
- [15] K. Jain and J. S. Baras, "Modeling traffic burstiness due to olsr routing and 802.11 mac in manets," in *pre-print*, 2013.
- [16] A. Feldmann, A. C. Gilbert, and W. Willinger, "Data networks as cascades: investigating the multifractal nature of internet wan traffic," in *Proceedings of the ACM SIGCOMM*, 1998.
- [17] D. Veitch and P. Abry, "A wavelet based joint estimator of the parameters of long-range dependence," *IEEE Transactions on Information Theory*, vol. 45, no. 3, pp. 878–897, 1999.
- [18] OPNET Modeler, http://www.opnet.com/solutions/network_rd/modeler.html.
- [19] G. Bianchi, "Performance Analysis of the IEEE802.11 Distributed Coordination Function," *IEEE Journal on Selected Areas in Communications*, vol. 18, March 2000.
- [20] A. Kumar, E. Altman, D. Miorandi, and M. Goyal, "New Insights from a Fixed Point Analysis of Single Cell IEEE 802.11 WLANs," in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, 2005.
- [21] J. S. Baras, S. Perumal, V. Tabatabaee, K. Somasundaram, and P. Purkayastha, "Loss Network Models and Multiple Metric Performance Sensitivity Analysis for Mobile Wireless Multi-Hop Networks," in *Fourth International Wireless Internet Conference*, 2008, pp. 60:1–9.
- [22] A. Jindal and K. Psounis, "The achievable rate region of 802.11-scheduled multihop networks," *IEEE/ACM Trans. Netw.*, vol. 17, 2009.
- [23] J. S. Baras, V. Tabatabaee, and K. Jain, "A model based platform for design and optimization of multi-hop 802.11 wireless networks," in *The Eighth ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks*, 2011, pp. 17–24.
- [24] J. S. Baras, V. Tabatabaee, G. Papageorgiou, and N. Rentz, "Performance Metric Sensitivity Computation for Optimization and Trade-off Analysis in Wireless Networks," in *Proceedings of the IEEE Global Communications Conference*, 2008, pp. 4884–4888.
- [25] J. S. Baras, V. Tabatabaee, P. Purkayastha, and K. Somasundaram, "Component based performance modeling of the wireless routing protocols," in *IEEE ICC Ad Hoc and Sensor Networking Symposium*, 2009, pp. 396–401.
- [26] J. S. Baras, V. Tabatabaee, and K. Jain, "Component based modeling for cross-layer analysis of 802.11 mac and olsr routing protocols in ad-hoc networks," in *Proceedings of the 28th IEEE conference on Military communications*, ser. MILCOM'09, 2009, pp. 1240–1246.